USAID Guyana
Democratic Consolidation
and Conflict Resolution
(GDCCR) Project

Voter Registration Cleanup Options: Report for Guyana Elections Commission

January 2005
This publication was produced for review by the United States Agency for International Development. It was prepared by Michael Yard, consultant to Research Triangle Institute and the Guyana Democratic Consolidation and Conflict Resolution Project.

Voter Registration Cleanup Options:
Report for Guyana Elections Commission

Prepared for
USAID Guyana Democratic Consolidation and Conflict Resolution Project
United States Agency for International Development

Prepared by
RTI International
3040 Cornwallis Road
Post Office Box 12194
Research Triangle Park, NC 27709-2194

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

This report was prepared by Guyana Democratic Consolidation and Conflict Resolution (GDCCR) Project at the request of the Guyana Elections Commission (GECOM) to provide options on the use and experience of "automated fingerprint identification systems" (AFIS).

Background on AFIS

How it works

Biometric systems are designed to identify persons based upon unique physical characteristics. The most common biometric system in use is automated fingerprint identification systems or AFIS. An AFIS system relies on the uniqueness and invariable nature of fingerprints over the lifetime of each person. The three stages of this system include fingerprint capture, feature extraction, and matching.

The fingerprint capture process is typically done using a live scanner. A typical standard digitizes fingerprints at 500 dots per inch producing a graphic image. The advantage of the live scan over prints based on ink and paper is that the system gives immediate feedback upon the quality and consistency of the fingerprints captured.

The extraction process involves identification of unique features of the print based upon its location (x, y coordinates) and the direction of the ridges at that location. The number of such features extracted, also known as minutiae, is decided during the system design process and has direct impact upon both the accuracy and the speed of the recognition system.

In the matching process the system compares the captured print with all the other prints stored in the database and arrives at a score indicating the degree of similarity between the prints. This score is then compared to a user defined threshold. If the score is higher than the threshold the system reports a possible match.

Inherent Limitations

Perhaps the greatest problem with automated fingerprint systems is the wide gap between the expectations placed upon the system and the reality of the system's capabilities. A common myth in the early days of computing was that "computers do not lie". There was a widespread belief that information coming out of the computer was inherently more accurate than non computerized information. With the increased availability of computers over the past three decades of this myth has crumbled under a new awareness that the information produced by a computer is only as accurate as the information fed into the computer, a reality commonly referred to as "garbage in, garbage out".

Unfortunately, it is still common for humans to have unrealistic expectations about the capabilities of the newly emerging technologies. The realities of automated fingerprint identification systems are reflected in a report of the National Task Force on Interstate Identification to the U.S. Attorney General, which claims that “modern automated fingerprint identification systems are believed to produce identification error rates of less than 1%”. Before placing too much trust in an AFIS system we should understand the reason for this error rate and its implications for the proposed usage.

Going back to the premise behind a fingerprint identification system, it is true that no two fingerprints are exactly the same. Unfortunately this is the case even if the two prints come from the same finger. Factors such as the orientation of the finger, elasticity of human skin, dirt, oils, abrasions, etc. all come into play with every fingerprint recorded. On the other hand, although it is true that no two human beings have identical fingerprints, many fingerprints will share some common characteristics. These two realities are manifested in the two types of errors in an automated fingerprint identification system, namely false acceptance and false rejection. False acceptance occurs when the system erroneously identifies two prints as coming from the same person. False rejection is when the system fails to recognize that two separate prints were both made by the same finger. The rate of error in an automated fingerprint identification system is expressed in the rates of these two types of errors, false acceptance rate (FAR) and false rejection rate (FRR). The FAR can be reduced by raising the threshold required for considering two prints a match, but any decrease in the FAR is accompanied by an increase in the FRR, and vice versa.

Now, an overall error rate of “less than 1%” does not render the system unusable, however it does limit the applications for which the technology is appropriate.

Additional Limitations

Widespread deployment of AFIS creates additional possibilities for human error or deliberate manipulation. Without adequate quality control and scrutiny, it would be possible for a registrar to capture fingerprints in the wrong order, or to capture the wrong person’s prints. Further, the AFIS database could be subject to the same kinds of problems as any other database, including data corruption or loss or even deliberate alteration. As with any computerized information system, the quality of the results can never exceed the quality of the base data.

Uses for AFIS

The two common applications for AFIS are authentication and identification. In an authentication application, the system answers the question, “Is this person who s/he claims to be?” Typically, the subject of the query will present an ID card or some other form of identification, and will then submit a finger for scanning. The system looks up the subject’s record in the database, and then compares the current fingerprint with the one on record. This is also known as 1:1 or one-to-one matching because the system is only comparing a newly captured fingerprint with a known fingerprint. In this case, there is a very low mathematical probability of an imposter having a fingerprint that is very similar to the person whose identity is on record, so the threshold in this kind of application is usually set low enough to prevent false rejection.

In an identification application, the identity of the subject is unknown, and the system must compare a newly captured fingerprint with all fingerprints in the database. This is also known as 1:N or one-to-many matching. In this application, the threshold can start low to prevent false rejection. If the system detects too many possible matches to allow manual comparisons, the threshold is gradually raised until a manageable number of matches are found. This application is typically used in law enforcement to allow officials to identify possible suspects in a crime investigation.

There have been many attempts to extend the capabilities of AFIS to N:N, or many-to-many matching, with relative degrees of success. In this type of application, every fingerprint in the system is matched against every other fingerprint in the system to detect duplicates. In order to implement such a system, the threshold must be set low enough to prevent an impractically high false acceptance rate (FAR). However, as explained above, any increase of the threshold will result in a corresponding increase in the false rejection rate (FRR).

A further, and even more consequential problem is inherent in an attempt to implement many-to-many matching. An AFIS system typically captures between 12 and 16 points of minutiae (unique identifying features). Therefore, a single one-to-one comparison of prints in fact involves 12 to 16 comparisons. When we extend this to one-to-many matching, it follows that the actual number of comparisons is not equal to the number of prints on record, but rather to that number multiplied times the number of minutiae captured.

Extending the previous calculation to accommodate a database of 500,000 persons, a one-to-many match against a database of 500,000 prints with 12 points of minutia would require 6 million comparisons (500,000 X 12). This is made possible by the tremendous speed of modern computers that are capable of doing thousands of comparisons per second. For example, the National Registration Database of Pakistan claims to have the fastest matching engine available, capable of matching up to 7,000 fingerprints per second based upon 14 points of minutiae. In this example, if we had a single fingerprint that we needed to compare to all other fingerprints in the system, the search/compare would take approximately 71 seconds (500,000 prints / 7,000 comparisons per second).

Implication for Voter Registration Systems

Using this number as a basis, we can project the time required to conduct a many-to-many match, comparing a database of 500,000 fingerprints against itself as follows:

Matches per second	7,000
Number of persons in database	500,000
# of seconds required for 1:N match	71
# of seconds required for N:N match	35,500,000
# of hours required for N:N match	9,861
Weeks required (48 hour work week)	205

Given a potential error rate of 1%, if we set the threshold low enough to eliminate any possible false rejections, we could end up with an average of 5,000 false acceptance hits per person. Obviously this would not yield any meaningful results, so we would be forced to raise the threshold in order to reduce the false acceptance rate to a practical level. In raising the threshold, however, we increase the false rejection rate, creating a significant possibility for persons to register multiple times without being discovered.

(NOTE: I believe the error rate is much lower than 1%, but use the rate projected by the report to the US Attorney General for purposes of illustration. Even with an error rate of .1% we could end up with an average of 500 false acceptance hits per person or a correspondingly high false rejection rate that would allow duplicate registrations.)

Options for Cleaning Voter Registry

Types of Problems to be Addressed

Guyana is not unique in the problem of maintaining an accurate voter register. Generally speaking, the problems that can occur in any voter register, and may be reflected to varying degrees in Guyana, include:

- Duplicate registrations, either by accident or by fraudulent intent
- Deceased persons still on electoral roll
- Persons on the roll who are not legally eligible
- Voters assigned to wrong Electoral Area or wrong Polling Station
- Under-registration of segments of the population, usually women, young voters, and minorities
- Misspelled names
- Incorrect details including address, gender, and age

All of these inaccuracies can have a negative impact on the ability to conduct free and fair elections, and even when the inaccuracies are not significant enough to impact outcomes, they can have a detrimental impact on voter confidence in the fairness of the electoral process.

Summary of Options

There are at least three options available for cleaning up the voter registration data, each with relative advantages and disadvantages:

- A new door-to-door registration exercise
- Claims and Objections process
- Required confirmation by positive affirmation

The first option, a new door-to-door exercise would have the advantage of eliminating all current inaccuracies and starting afresh. The disadvantage is that we are "throwing the baby out with the bathwater", by also eliminating all accurate data currently in the database and incurring a major expense to recreate that data.

The second option, Claims and Objections process, is currently mandated by law in Guyana and consists of public display of the list, providing all concerned parties to scrutinize the list and submit a claim for correction of their own data, or object to the inclusion of anyone they consider ineligible to appear on the list. The advantage is that this is the most cost-effective approach, maintaining a focus on correcting errors rather than re-entering all data. The disadvantage is that there is usually very low interest by voters to inspect the list, and inadequate time for political parties and NGO's to do a thorough inspection.

The final option is similar to the Claims and Objections process currently used prior to elections in Guyana, however all voters are required to appear at a registration center to confirm the accuracy of his/her data by signature, either on the list itself or on a separate form. Any person who fails to affirm the accuracy of his/her data is purged from the list of voters. This is an effective way to remove the deceased and those who have relocated, either to another electoral area or out of the country. However, this requirement places the greatest burden on those segments of the voter population who are already likely to be underrepresented, namely the poor, the uneducated, those in remote areas, and possibly female voters who may be less mobile than their male counterparts.

Criterion: One Person, One Vote

The decision on which approach to use must be based upon a careful weighing of cost, schedule, and real benefit to the election process. The purpose of a voter register is to enable every eligible voter to have equal voice in the decisions being voted upon, while disallowing all who are not eligible. A voter register alone cannot accomplish this – in fact, an election based upon a faulty register that is conducted in an open and transparent manner, under careful scrutiny of party representatives and impartial observers is preferable to an election based upon a perfect register, but conducted in a way that obscures scrutiny by observers.

In an open and transparent process every voter is subjected to the scrutiny of an electoral officer, as well as agents from political parties and impartial observers. The voter register is only one level of control since the voter must prove his identity to the satisfaction of all of these scrutineers before being allowed to vote. In addition, measures are put in place such as use of ink on the fingernail to prevent this person from voting again in another polling station. In this system there is a reasonable level of control to guarantee that only those persons who are eligible are allowed to vote, and that each eligible voter is allowed to vote only once. Finally, the presiding officer at the polling station must account for every ballot received, and the total number of votes plus spoiled ballots plus unused ballots must be equal to the number of ballots received. In such an environment the problem of an outdated voter list that includes deceased persons or those who have emigrated is minimal, since the system guarantees the "one person, one vote" principle. The greater risk of a faulty voter list is that some voters may be disenfranchised by have a name erroneously omitted from the list.

Contrast this with a process that has a perfect list but inadequate scrutiny and accountability. In this system any person can show up and pose as a voter whose name is on the list and the authentication of this person's identity is at the sole discretion of the electoral officer. Without adequate scrutiny any person can be allowed to vote, regardless of whether his name appears on the list, without having ink applied to his finger, and indeed any voter could be allowed to cast multiple votes. Without the added accountability of ballots, every polling station would have the option of stuffing ballot boxes by marking unused ballots. Clearly, the voter register is only one part of a clean electoral process and it bears repeating that an election based upon a faulty register that is conducted in an open and transparent manner, under careful scrutiny of party representatives and impartial observers is preferable to an election based upon a perfect register, but conducted in a way that obscures scrutiny by observers.

Procedural recommendations

This is not to say that GECOM should be lax in its responsibility to produce a clean and accurate voter list, only that an over-emphasis on the list may obscure the focus on the main goal of ensuring the "one person, one vote" principal. The following steps can provide significant improvement to the current process of maintaining the voter register:

1. Continuous Registration - GECOM secretariat has already done much work preparing for a process of continuous registration, and this process should remain a central focus for cleaning up the voter register. GECOM alone cannot create an accurate voter register, regardless of any technology it may decide to implement! By providing voters and parties an opportunity to continuously scrutinize the voter lists, and to submit claims and objections at any time, GECOM will have appropriately shared the responsibility for improving the accuracy of the register.

2. Photo Voter List - As previously suggested, a further enhancement to the registration process that can aid in the scrutiny of the voters list is the addition of a photo to the list itself. With this addition not only would the voter be required to show a photo ID to the electoral officer and scrutineers at the polling station, but the voter's photo would be displayed where it could be viewed by every other voter, and parties would have adequate time to scrutinize every voter appearing on the list prior to any election. This measure would provide a strong deterrent against any attempt to register fraudulently.

3. Regular Feedback Process - Finally, it is important that feedback be given to registration offices, and to political parties on all changes made to the voter register. If an individual voter submits a claim for modification of his/her record there should be a clear accounting that this claim has been handled accurately. Similarly, if an individual or party lodges a successful objection to any name appearing on the list, there should be a clear accounting that the name has been removed. This can best be accomplished by issuing regular reports, broken down by registration center that itemize all changes. These changes should be grouped by Additions, Removals, and Corrections, with a summary total of all changes made and the number of voters now on the revised register. This will allow all interested parties to closely monitor every change made, allowing for a completely transparent process of continuous improvement.